BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

GP. 3642
#4
KW
1499

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

JOHAN P. LINNARTZ

Serial No.: 09/013,541

Filed: JANUARY 26, 1998

Title: SYSTEM FOR COPY PROTECTION OF RECORDED SIGNALS

Atty. Docket No.

PHN 16,210

Group Art Unit: 3642

Honorable Commissioner of Patent and Trademarks
Washington, D.C. 20231

CLAIM FOR PRIORITY

Sir:

A certified copy of the EUROPEAN Application No. 97200165.5 filed JANUARY 27, 1997, referred to in the Declaration of the above-identified application is attached herewith.

Applicant claims the benefit of the filing date of said EUREOPEAN application.

Respectfully submitted,

APRIL 20, 1998
Enclosure

By Michael E. Belk
Michael E. Belk, Reg. 33,357
Attorney
(914) 333-9640

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:
COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

On 4/22/98

By Michael E Belk

S:\BE\MV20BEL0.SW0

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

97200165.5

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

M.W. Graham

DEN HAAG, DEN
THE HAGUE, 17/02/98
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 97200165.5
Demande n°:

Anmeldetag:
Date of filing: 27/01/97
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
PHILIPS ELECTRONICS N.V.
5621 BA Eindhoven
NETHERLANDS

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
System for copy protection of recorded signals

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
G11B20/00

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

System for copy protection of recorded signals.

The invention relates to a system for copyprotection of recorded information, comprising an information carrier, a player and a recorder.

The invention further relates to an information carrier which comprises a track for writing patterns which represent information in a predefined manner and for writing related auxiliary information.

The invention further relates to a reading device for reproducing information from an information carrier, the information carrier comprising a track for writing patterns which represent information in a predefined manner and for writing related auxiliary information, the device comprising reading means for reading the patterns, and a demodulation means for recovering the information from the read signal in a predefined manner, and means for recovering the auxiliary information.

The invention further relates to a recording device for recording information on an information carrier

The invention further relates to a method of manufacturing an information carrier which comprises a track for writing patterns which represent information in a predefined manner and for writing related auxiliary information, the auxiliary information being determined in dependence on the information.

Such a system, information carrier and reading device are known from EP-0545472. The known information carrier comprises a prearranged guiding track, a so-called pregroove. In the track determined by the pregroove, information which is written in a predefined manner is represented in optically readable patterns which are formed by variation of a first physical parameter, such as the height of the scanned surface. The pregroove has variations in a second physical parameter, such as an excursion in transverse direction, also denoted as wobble. Pregroove wobble is FM modulated and this modulation represents auxiliary information which is related to the information such as, for example, a descramble code for recovering information stored

as scrambled information. The known device comprises reading means for reading the patterns and recovering means for recovering the auxiliary information. The known device and information carrier form a system for controlled information reproduction. For this purpose, the device comprises means for reproducing the information in dependence on the auxiliary information. If the information is copied on a writable information carrier, the information of this copy will not be reproduced, because during the writing process only the patterns are written and the copy itself does not contain any auxiliary information.

A problem in the known system is that copy protection is complicated.

It is an object of the invention to provide a system in which copy protection is accomplished in a convenient way.

For this purpose, the system according to the invention is characterized in that the recorded information comprises a specific bitpattern as watermark and in that the information carrier comprises a physical mark, and in that the player and the recorder comprise means for processing the specific bitpattern and the physical mark.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter.

It is to be noted, that the subject matter referred to as a watermarking method, proposed by A.A.M. Bruekers et al. and described in "Watermarking of Bitstream- or DSD-signals" as mentioned in chapter 7, Bibliography, is disclosed also in the copending European Patent Application of the same applicant on the same filing date, applicants reference PHN 16209.

Copy Protection method for storage media, DVD audio in particular

J.P.M.G. Linnartz
Philips Research Laboratories
Eindhoven, The Netherlands

January 23, 1997

Executive Summary

We propose a copy control method for bitstream- or DSD-signals stored on storage media such as DVD audio. The method relies on a watermarking method, such as the one proposed by A.A.M. Bruekers et al.

1 Introduction

Copy protection has a long history in audio publishing. The installed base of equipment, including PC's with audio cards, provide little protection against unauthorized copying. In any copy-protection scheme, the most difficult issue is that a pirate can always attempt to playback an original disc, he can treat the content as if it were an analog home recording and record this. Consumer recorders should be able to make recordings of customer's own creative productions without any limitation, but prohibit the recording of copy-righted material. Thus, the copy protection mechanism must be able to distinguish between customers' own creations and content that originates from professional music publishers. The equipment must make this distinction based on the content only, as any reference to the physical source of content (e.g. disc or microphone) is unreliable. For digital storage media such as DCC, "copy bits" have been defined. Recently, it has been realized that watermarks or embedded signalling can be used to make copy protection methods more robust against attacks. Embedded signalling or watermarking is a method of burying information in the audio content.

In this text we use the word *professional* for any product that is officially registered with a trusted party which represents the interests of the recording industry and hardware manufacturers. We denote any other product as a *consumer* product.

Consumer products are assumed to obey copyright rules, enforced either by a patent licencing agreement or by law, or both.

1.1 Is a total Copy Protection solution within reach?

Watermarking is not restricted to digital formats, but can also be embedded and detected in analog signals. Often, spread-spectrum technology is proposed for embedding watermarks into audio (see e.g. U.S. patent 5,319,739). A technical difficulty of spread-spectrum methods is that retrieval or detection of such embedded data requires substantial signal processing. Although this is not a problem for professional equipment used in legal cases to prove the origin of the audio material, the computational effort appears far beyond what is feasible and economically reasonable within comsumer electronic products to support copy protection. A particular problem is that the audio quality requirements set by the music industry would require such large spreading gains that synchronization and data detection would take excessively long integration times. Parameters considered in U.S. patent 5,319,739 presumably do not satify current audio quality requirements. Future standards aim at further enhancing the audio quality and simultaneously require secure protection of music IPR. It is our strong belief that it is unlikely that satisfactory methods will indeed be found in near future to combine these two requirements at reasonable cost.

Particularly the absence of protective measures in the installed base of audio equipment causes a problem. It appears virtually impossible to avoid that signals can be copied by going back to analog. Moreover, consumer expectations are that some kind of home taping, e.g. to listen in the car, should be possible. On top of that, in some countries that levy a fee on blank tape for analog copying for private use, certain technical means to restrict analog copying are not legally acceptable.

There appears an opportunity to set new standards for storage and representation of digital audio (e.g. DVD), but technology to solve the copy protection issue completely (i.e., including analog copying) is unlikely to become available soon.

1.2 Is a bitstream-only solution of any use?

Given this situation, it can be useful to protect new audio storage media against "Chinese" copying of discs, even if analog copying remains possible. In order to copy, conversion into other domains (e.g. analog) are needed and some loss of quality occurs. The scheme proposed here does not solve the existing problem of piracy and excessive home taping whereby the audio signal is converted to analog as part of the copy process.

If the industry adopts a copy protection scheme based on watermarking, it will presumably come to a layered approach. The most robust watermark should withstand D/A and A/D conversion, but this will require long integration times for the de-

tection. This implies that the record or playback inhibit decision will be delayed. A watermark in the bitstream can be detected within milliseconds and trigger copy protective measures immediately. Such fast detection appears essential if bitstream signals are transferred over open busses (P 1394). In summary, the method described in thgis documenthas the follwing properties.

- Bitstream or DSD signals with copy-right restrictions can immediately be distinguished from home recordings.
- Tracability of the professional or consumer recorder.
- It can co-exist with other methods that also protect against other forms of copying (e.g. analog). In particular, it appears of interest to add conditional playback using the method proposed here to a conditional recording method which also checks for spread spectrum watermarks.

2 Protecting Bitstream or DSD

We propose a scheme that protects against direct (bitwise) copying of high quality digital DSD streams. The method does not technically protect against conversion of DSD to PCM or analogue. However, some protection is provided against such attacks in the sense that if a bitstream / DSD signal, it is converted back into DSD will be watermarked with the serial number of the consumer DSD encoder.

The method relies on a watermarking method, such as the one proposed by A.A.M. Bruekers et al. Our method can coexist with many other forms of copy protection, including serial copy management bits and the embedded signalling described in U.S. patent 5,319,739. The additional hardware in consumer equipment appears very small.

Another tool used in the system scenarios to be described in the next chapter is a medium mark, i.e., a method to distinguish a professionally mastered disc from a recordable. Implementations of such tool can be a wobble key (Philips), modulation of EFM[P] errors (e.g. HP) intentionally modulation the jitter of pits and lands of a disc (e.g. SONY) embedding an on-disc chip (e.g. TI), or just data written in the lead-in area which is not accessable by consumer recorders.

These two tools (watermark and medium mark) are used to support the following features (both or just one):

Conditional recording is the most commonly known method for copy protection. A consumer recorder will not record material unless it it sure that the material may indeed be copied legally.

Conditional playback, on the other hand, accepts that some people will be able to get the bits of copy-righted DSD on a pirate disc anyhow. Conditional playback will

make sure that such a pirate disc can not playback on consumer players. That is, pirates cannot commercially distribute illegal copies.

3 Conditional playback

In conditional playback, a consumer DVD audio player will only play audio discs if certain copyright conditions are met. The player identifies the audio content either as a consumer recording or as professionally published audio content, by detecting or checking for a watermark in the audio stream. In the latter case (professional content protected by copyright), the player checks whether the physical disc is original and professionally mastered, rather than a copy on a consumer recorder or consumer disc press. This requires both a marking method for the content (watermarking) and a method for marking the physical storage medium that can only be produced by a professional recorder or pressing machine.

Physical mark:	Consumer	Professional
Audio Watermark	play	play
No Audio Watermark	block	play

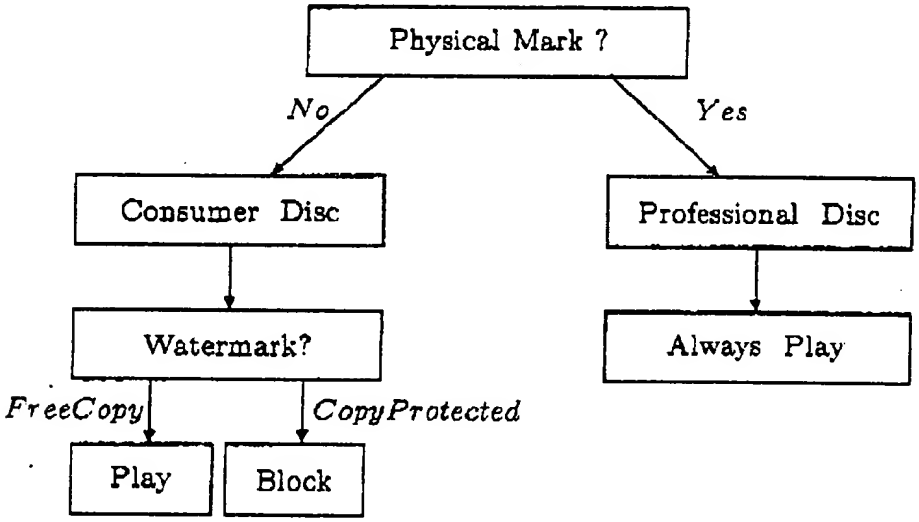


Figure 1: *Conditional playback rules*

3.1 Copy Control Scenario 1.a

Professionally mastered audio discs carry an identifier unique to the publisher, which can not be copied. This identifier can for instance be a set of bits written in an area

that is not accessible for recorders, it can be a wobble key or a special pattern in the running DC component of the EFMP code. The DVD audio player checks for this mark. If this mark is unavailable or if it contains a special code reserved for home disc recorders, it will only playback the DSD stream if a special watermark is found that identifies the DSD encoder. If this watermark is not found, as would be the case if a professionally released audio stream is copied illegally to a recordable disc, the audio is not played back at all.

To avoid any degradation of the quality of professional DSD releases this scenario does *not* require that the audio content of professionally released audio titles is watermarked, but this scenario requires that the watermark embedding method is used in consumer equipment. Besides a frequently repeated copy control bit, a unique serial number is embedded into the audio stream by all DSD encoders/recorders in the consumer market. The circuitry to embed this number appears simple.

The consumer can not copy professional DSD audio directly to a DVD audio disc, as it will not playback (because of the watermark be absent). If he converts the signal to analog, PCM or another format, and then re-creates DSD, the particular DSD recorder can be traced. Moreover, the scheme can be defined in such a way that home recordings have smaller dynamic range [See the proposal by Bruekers what the effect of watermarks is on audio quality].

A further strengthening is achieved if each player not only checks whether a watermark is present on comsumer discs, but also check whether a *valid* serial number is embedded. Known cryptographic methods can be used for integrety checks, e.g. concatenating a digital signature to the serial number. This avoids that a pirate can tamper with serial numbers.

3.2 Copy Control Scenario 1b

This is similar to scenario 1.a, but the bit stream of professionally released audio does also contain a watermark. This watermark is used to verify the medium mark in a cryptographic way. The medium mark now differs from title to title.

Let $y = F(x)$ and $x = G(u)$ be two cryptographic one-way functions, i.e., their inverse is computationally infeasible to compute with finite arithmatic resources. This scenario uses a seed u to create x and y, according to $x = G(u)$ and $y = F(x) = F(G(u))$. In this concept G and F may be the same function, but this is not necessary. On a professionally mastered disc, the embedded watermark contains y and the medium mark carries x. Professional recorders always perform the G function before writing a medium mark. That is, they embed a medium mark x which is internally generated from the user input u. All (consumer) players perform F to verify the medium mark if a watermark is found that indicates that the content is copy protected. Consumer recorders are assumed not to be able to write a medium mark at all.

The copy-right owner can decide himself whether or not to release the seed u, which

allows copying. In professional music publishing, it can be necessary to create a tape master of the music title. The audio is then pre-encoded with embedded the watermark y. During the production process, the professional recorder (disc master generator machine) directly accepts the watermarked DSD and inserts this after the DSD encoder/watermarker of Figure 1. Seed u is also inserted during this process. This also provides some protection if the master tape is stolen, but u is not compromised. Preferably, the recorder checks the watermark against u and x (see: conditional recording).

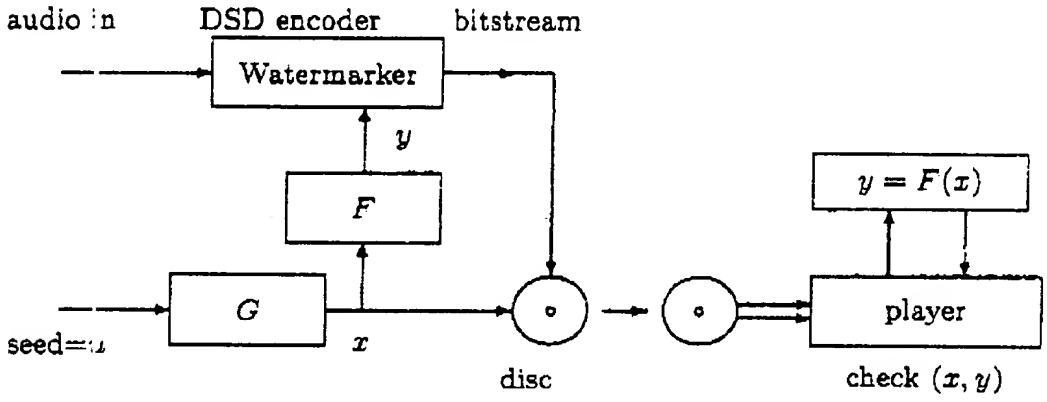


Figure 2: *Conditional playback scenario 1.c. Professional Recorder and consumer player*

In this scenario, a pirate must have access to a compromised professional recorder to create media marks on a pirate disc. A pirate can copy the audio and recover y, but he cannot calculate x. This system adds security to the copy protection scheme, particularly if we can ensure that x cannot easily be read from the disc, i.e., remains within the first chip in the basic engine (that must use x to verify watermark y). Moreover, even if a pirate can read x, he must find u to enter it into the recorder and to have x written as medium mark. No recorder will directly accept to x and write it to disc. In this scenario, a pirate must physically modify both his (officially registered mastering) recorder (to bypass the G function) and his player (to extract x).

3.3 Providing copy protection for consumer recordings

It can be envisioned that consumers want to publish or disseminate their own recorded audsio creations at a small scale. We now describe how consumer recorders can implement some of the elements of the above scheme. This gives consumers the possibility to create discs that can only be copied directly (bit-by-bit) if the receipient also knows seed u.

A possible extension is split x into two parts, with $x = x_1||x_2$, such that $y = F(x_1||x_2)$. Then x_1 acts as a medium mark, similar to the scenario described above, and x_2 is written as a separate file on the disc. Professional recorders can write x_1 as well as x_2. Consumer recorders can write x_2 but on recordable discs, x_1 has a default value $x_1 = x_c$ prepressed on the disc. The consumer recorder embeds watermark $y = F(x_c||x_2)$ where x_2 is generated from a seed u, i.e., by taking a portion of the bits of $G(u)$. The owner can copy his own creations because he knows u.

In players, neither x_1 nor x_2 leaves the basic engine, so it remains hidden for the user.

3.3.1 One-way functions

An implementation of the one-way function can be $y = x^2 \mathrm{mod} N$ with N a public modulus. Here N is the product of two secret large primes ($N = pq$). In fact N can be part of the data that is embedded in the watermark, i.e., concatenated to y.

Another possibility is the discrete-log one-way function conjectured by Diffie and Hellman [1976]: $F(x) = \alpha^x$ in $GF(p)$ with α a primitive element of $GF(p)$. Here p is a large prime such that $p - 1$ has a large prime factor.

The above two implemenations bear the disadvantage that the size of the arguments, i.e., the number of bits needed to be secure, is quite large. A practical system based on fewer bits can be to apply an appropriate secret-key encryption algorithm, e.g. the DES, with $y = F(x) = x \otimes \mathrm{DES}(x)$. This is illustrated in the circuit of Figure 3. In this circuit, the key is made public or included in the watermark, i.e., concatenated to y.

4 Conditional Recording

In its pure form, the conditional recording scenario does not perform checks during playback. A consumer DSD recorder accepts an analog signal, possibly conditional to some analog copy information check. An on-board DSD encoder embeds a watermark into the stream. This mark consists of two parts: copy protection data and a serial id. number of the recorder. The consumer DSD recorder accepts a digital DSD stream only if it can recognize valid copy control data. This copy control data

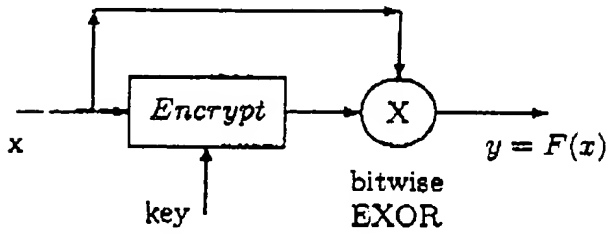


Figure 3: *One-way function based on secret-key encryption algorithm*

should state that this material may legally be copied onto a disc.

The consumer DSD recorder does not accept a DSD stream that contains Copy Control Marks that prohibit recording. In its strongest form, the absence of Copy Control Information is interpreted as "no copy allowed". In a weaker form, signals without copy control information are automatically resampled and watermarked. This weakens the copy protection, but leads to some quality degradation.

4.1 Copy Once

A professional DSD stream can contain embedded copy-right data that grants permission to copy once. This can be implemented by embedding a watermark y_{co} (in addition to mark described earlier). Moreover the professional disc contains a special permission mark x_{co} where $y_{co} = H(x_{co})$ with $H()$ a cryptographic one-way function. The mark y_{co} remains with the audio (possibly embedded) during playback, but it is removed by the consumer recorder.

5 Hybrid Solutions

Conditional recording and conditional playback can co-exist.

5.1 Coexistance

Of particular interest is a scenario in which (despite technical difficulties described in the introduction) a watermark check in the analog domain should be performed by recorders.

If a pirate manages to modify his recorder to bypass this conditional recording check, and put professional DSD on a disc anyhow, the copy protection schemes described here can prevent playback on players in the market.

6 PCM audio

A form of watermarking is also possible for PCM audio, One example is hiding data in the LSB's, possibly including a spectral shaping of their effect. An implementation for such embedding scheme has been presented by Oomen et al. in 1994. For our application, we preferably would only embed data in a limited number of preselected samples, with one bit per selected sample. Such embedding scheme can be implemented within the same device that converts profesional (24 bit) audio into lower resolution (e.g. 16 bits) The method previously mentioned for DSD watermarking (by Brueker) potentially can also be used for embedding data in PCM.

Another option is to use the loss-less encoding for embedded signalling. One method for lossless encoding was proposed by Bruekers, Oomen, vd Vleuten en vd Kerkhof at the 1996 AES Convention ("Lossless coding for DVD audio"). A possible method of embedding data is by choosing the properties or parameters of the predictive filter (Fig. 2 of the AES paper) in accordance with watermarking rules. For instance, a digital watermark "1" can be represented by choosing an even number of filter taps and a "0" is represented by an odd number of taps. In another implementation, the filter coefficients are quantized according to a similar rule. Further, the entropy encoder can embed data by adapting its parameters.

Such signals embedded into the PCM signal can be used to build a copy protection scheme based on any of the previously mentioned concepts. A pirate can no longer copy the compressed PCM bit-by-bit onto a disc that he can distribute commerically. He must go through the process of decompression and compression. Although this does not lead to a degradation in quality (because the coding is loss-less),

- it results in a different digital signal
- the resulting file will contain more bits if consumer recorders can compress less efficiently
- the resulting file will contain information about the serial number of the recorder.

7 Bibliography

Watermarking of Bitstream- or DSD-signals, A.A.M. Bruekers, G.F.G. Depovere, P.A.C. Nuijten and A.W.J. Oomen, witte kaart, Dec 1996

A.W.J. Oomen et al. "A variable bit rate buried data channel for compact disc" 96th AES Convention, 1994, Amsterdam.

11

Copy Protection

for DSD and PCM audio

J.P. Linnartz/ January 23, 1997

Philips
Research

PHILIPS

Objectives

- Protective measures both during playback and recording
- Copy Protective measures should be inaudible
- Recorders should be tracable
- Semi-professional and home audio recording of user's own creations should be possible, using the same audio formats.

Basic Principle

All discs carry

- a medium mark, e.g. a wobble key, timing jitter, ..
  - 64 bits key x_c identifying the publisher

    fixed for each disc mastering machine / press

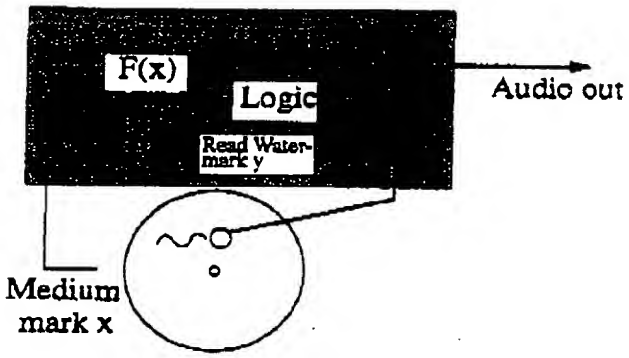
    default value for recordables
  - 64 bits key x_t identifying the title

    generated from a user definable seed u, with $x_t = G(u)$
- DSD audio with watermark y, $y=F(x_c||x_t)$
- PCM audio with watermark y, $y=F(x_c||x_t)$

$F()$ and $G()$ are publicly known cryptographic one-way functions

Basic Principle: Playback Control

- During playback, the player checks whether $y=F(x_c||x_t)$
- Playback is blocked if mismatch



Basic Principle

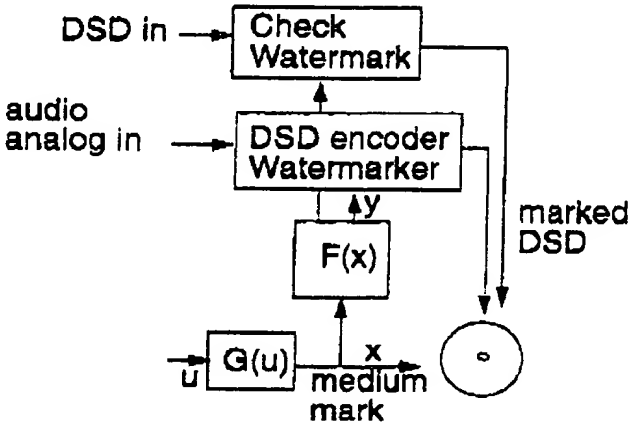
Basic Principle: Recording Control

- Before / during recording, consumer device checks for watermark in PCM and DSD audio signals

  No recording if professional "no-copy" watermark is present

  Embed watermark if none is present

- Analog: digitize with watermark/serial number



- Similar for recording PCM

Watermarking methods: DSD

- 0.1% or less of the DSD bits carry watermark data
- Large bandwidth for embedded signalling
- Inherent shaping of watermark noise to inaudible frequencies
  - Watermark artefacts are removed from audio spectrum by noise shaping
  - SNR decreases 1 dB if 1% of bits is used for watermarking
- Watermarks can very easily be read for DSD signal
- Removing the watermark requires conversion to other format (e.g. D/A conversion)
- Consumer recorder can embed watermark, serial number etc. into audio stream.

Watermarking methods: PCM

- Option 1: Watermark is part of loss-less coding
  - No artefacts at all (loss-less!)
  - Data vanishes after loss-less decompression
- Option 2: Adaptive data hiding in LSB of particular samples (recommended)
  - Artefacts are small.
  - Data vanishes after D/A conversion or digital filtering
- Option 3: Adaptively shaped spread-spectrum signal is added (not advised)
  - Robust against D/A conversion
  - Expensively expensive hardware (spread-spectrum receiver)
  - Slow detection of embedded data
  - Audible artefacts

Copying after conversion to Analog

- Remains possible
- Recorder is traceble
- Degradation of quality
- Our proposal can be compatible with schemes that protect against analog copy protection, when available

Copy-Once

- Currently under study

CLAIMS:

1. System for copyprotection of recorded information, comprising an information carrier, a player and a recorder, characterized in that the recorded information comprises a specific bitpattern as watermark and in that the information carrier comprises a physical mark, and in that the player and the recorder comprise means for processing the specific bitpattern and the physical mark.

2. System for copyprotection of recorded information, as described in the accompanying description.